10/089646

R E P U B L I Q U E F R A N Ç A I S

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 05 AVR. 2002

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

CERTIFIED COPY OF
PRIORITY DOCUMENT

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (1) 53 04 53 04
Télécopie : 33 (1) 42 93 59 30
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Telephone : 01 53 04 53 04 Télecopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

RÉCÉPISSÉ DE DÉPÔT

Confirmation d'un dépôt par télécopie ☐

A remettre au demandeur ou au mandataire

Réservé à l'INPI

DATE DE REMISE DES PIECES - 1 OCT. 1999

N° D'ENREGISTREMENT NATIONAL 9912468

DÉPARTEMENT DE DÉPÔT

DATE DE DÉPÔT 01/10/1999

I: N. P. I: RENNES

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Patrice VIDON
Cabinet Patrice VIDON
CENTRE D AFFAIRES LE NOBEL BAT A
2 ALLEE A BECQUEREL BP 90333
35703 RENNES CEDEX 7

n°du pouvoir permanent | références du correspondant | téléphone
5972 | 02.99.38.23.00

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ demande initiale

☐ certificat d'utilité ☐ transformation d'une demande de brevet européen ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☐ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Procédé destiné à prouver l'authenticité d'une entité ou l'intégrité d'un message au moyen d'un exposant public égal à une puissance de deux .

3 DEMANDEUR (S) n° SIREN code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination — Forme juridique

1. **FRANCE TELECOM** — **Société Anonyme**
2. **TELEDIFFUSION DE FRANCE** — **Société Anonyme**
3. **MATH RIZK** — **SPRL (Société de droit belge)**

Nationalité (s) Française

Adresse (s) complète (s) — Pays

1. **6 place d'Alleray, 75015 PARIS** — **France (1,2)**
2. **10, rue d'Oradour-sur-Glane, 75732 PARIS Cédex 15** — **France (1,2)**
3. **Verte Voie, 20 – Boîte 5, B-1348 LOUVAIN-LA-NEUVE, Belgique** — **Belgique (3)**

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☐ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande
France	99 01065	27 janvier 1999	
France	99 03770	23 mars 1999	

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

P. VIDON
(CPI 92-1250)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

BA 540 E 200298

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL

99 12 468

TITRE DE L'INVENTION :

Procédé, système, dispositif destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

LE(S) SOUSSIGNÉ(S)

Patrice VIDON
Cabinet Patrice VIDON
Immeuble Germanium
80 avenue des Buttes de Coësmes
35700 RENNES

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

M. Louis GUILLOU
16 rue de l'Ise
35230 BOURGBARRE
FRANCE

M. Jean-Jacques QUISQUATER
3 avenue des canards
B-1640 Rhode Saint Genèse
BELGIQUE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

le 1er octobre 1999
P. VIDON (CPI 92-1250)

BA 113/140897

DOCUMENT COMPORTANT DES MODIFICATIONS

* PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
1				29/11/99	16 DEC. 1999 - LB K

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifées).

Procédé, système, dispositif destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

La présente invention concerne les procédés, les systèmes ainsi que les dispositifs destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Le brevet EP 0 311 470 B1 dont les inventeurs sont Louis Guillou et Jean-Jacques Quisquater décrit un tel procédé. On y fera ci-après référence en le désignant par les termes : "brevet GQ" ou " procédé GQ". Par la suite on désignera parfois par "GQ2", "invention GQ2" ou "technologie GQ2" la présente invention.

Selon le procédé GQ, une entité appelée " autorité de confiance " attribue une identité à chaque entité appelée " témoin " et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : " *Voici mon identité ; j'en connais la signature RSA.* " Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée " contrôleur " vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant le procédé GQ se déroulent " sans transfert de connaissance ". Selon le procédé GQ, le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

La technologie GQ précédemment décrite fait appel à la technologie RSA. Mais si la technologie RSA dépend bel et bien de la factorisation du module n, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites "multiplicatives" contre les diverses normes de signature numérique mettant en oeuvre la technologie RSA.

L'objectif de la technologie GQ2 est double : d'une part, améliorer les

performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La connaissance de la clé privée GQ2 est équivalente à la connaissance de la factorisation du module n. Toute attaque au niveau des triplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 évite les inconvénients présentés par la technologie RSA.

Le procédé GQ met en œuvre des calculs modulo des nombres de 512 bits ou davantage. Ces calculs concernent des nombres ayant sensiblement la même taille élevés à des puissances de l'ordre de $2^{16} + 1$. Or les infrastructures microélectroniques existantes, notamment dans le domaine des cartes bancaires, font usage de microprocesseurs auto-programmables monolithiques dépourvus de coprocesseurs arithmétiques. La charge de travail liée aux multiples opérations arithmétiques impliquées par des procédés tels que le procédé GQ, entraîne des temps de calcul qui dans certains cas s'avèrent pénalisant pour les consommateurs utilisant des cartes bancaires pour acquitter leurs achats. Il est rappelé ici, qu'en cherchant à accroître la sécurité des cartes de paiement, les autorités bancaires posent un problème particulièrement délicat à résoudre. En effet, il faut traiter deux questions apparemment contradictoires : augmenter la sécurité en utilisant des clés de plus en plus longues et distinctes pour chaque carte tout en évitant que la charge de travail n'entraîne des temps de calcul prohibitifs pour les utilisateurs. Ce problème prend un relief particulier dans la mesure où, en outre, il convient de tenir compte de l'infrastructure en place et des composants microprocesseurs existants.

La technologie GQ2 a pour objet d'apporter une solution à ce problème tout en renforçant la sécurité.

Procédé

Plus particulièrement, l'invention concerne un procédé destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n$$

Ledit exposant **v** est tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 .

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

Ledit procédé met en œuvre selon les étapes ci-après définies une entité appelée témoin. Cette entité dispose des **f** facteurs premiers p_i et/ou des

paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et de l'exposant public **v** .

Le témoin calcule des engagements **R** dans l'anneau des entiers modulo **n**. Chaque engagement est calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

où **r** est un aléa tel que $0 < r < n$,

- soit
  - •• en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$,

  - •• puis en appliquant la méthode des restes chinois.

Le témoin reçoit un ou plusieurs défis **d**. Chaque défi **d** comporte **m** entiers d_i ci-après appelés défis élémentaires. Le témoin calcule à partir de chaque défi **d** une réponse **D**,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

- soit
  - •• en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

  - •• puis en appliquant la méthode des restes chinois.

Ledit procédé est tel qu'il y a autant de réponses **D** que de défis **d** que d'engagements **R.** Chaque groupe de nombres **R, d, D** constitue un triplet noté **{R, d, D}.**

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le procédé selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une

entité appelée contrôleur. Ladite entité démonstrateur comprend le témoin. Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

• **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le démonstrateur transmet au contrôleur tout ou partie de chaque engagement **R.**

• **étape 2 : acte de défi d**

Le contrôleur, après avoir reçu tout ou partie de chaque engagement **R,** produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur.

• **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse **D** au contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où le démonstrateur a transmis une partie de chaque engagement **R,** le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou a une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Le contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** qui lui a été transmis,

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifie que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou a une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le procédé selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ladite entité démonstrateur comprend le témoin.

Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

- **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus.

- **étape 2 : acte de défi d**

Le démonstrateur applique une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**. Le démonstrateur transmet le jeton **T** au contrôleur. Le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur.

- **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse **D** au contrôleur. Le contrôleur, disposant des m valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque

défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Puis le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**. Puis le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée aux deux précédentes, le procédé selon l'invention 1 est destiné à produire la signature numérique d'un message **M** par une entité appelée entité signataire. Ladite entité signataire comprend le témoin.

Opération de signature

Ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D**.

Ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus.

- **étape 2 : acte de défi d**

Le signataire applique une fonction de hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour obtenir un train binaire. Le signataire extrait de ce train binaire des défis **d** en nombre égal au nombre

d'engagements **R.**

• **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

Opération de contrôle

Pour prouver l'authenticité du message **M**, une entité, appelée contrôleur, contrôle le message signé. Ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme suit.

• **cas où le contrôleur dispose des engagements R, des défis d, des réponses D,**

Dans le cas où le contrôleur dispose des engagements **R,** des défis **d,** des réponses **D** le contrôleur vérifie que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

Puis le contrôleur vérifie que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R)}$$

• **cas où le contrôleur dispose des défis d et des réponses D**

Dans le cas où le contrôleur dispose des défis **d** et des réponses **D,** le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D,** des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

Puis le contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R')}$$

• cas où le contrôleur dispose des engagements R et des réponses D

Dans le cas où le contrôleur dispose des engagements **R** et des réponses **D,** le contrôleur applique la fonction de hachage et reconstruit **d'**

$$\mathbf{d' = h\ (message, R)}$$

Puis, contrôleur vérifie que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$\mathbf{R \equiv G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . \bmod n}$$

Système

La présenté invention concerne également un système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $\mathbf{Q_1, Q_2, \ldots Q_m}$ et publiques $\mathbf{G_1, G_2, \ldots G_m}$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $\mathbf{p_1, p_2, \ldots p_f}$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$\mathbf{G_i . Q_i^v \equiv 1 . mod\ n} \text{ ou } \mathbf{G_i \equiv Q_i^v \bmod n} .$$

Ledit exposant **v** est tel que

$$\mathbf{v = 2^k}$$

où **k** est un paramètre de sécurité plus grand que 1 .

Ladite valeur publique $\mathbf{G_i}$ est le carré $\mathbf{g_i^2}$ d'un nombre de base $\mathbf{g_i}$ inférieur aux **f** facteurs premiers $\mathbf{p_1, p_2, \ldots p_f}$. Le nombre de base $\mathbf{g_i}$ est tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

Ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif témoin comporte une zone mémoire contenant les **f** facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public **n** et/ou les **m** valeurs privées Q_i et/ou les **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et l'exposant public **v** . Ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin.

Les moyens de calcul permettent de calculer des engagements **R** dans l'anneau des entiers modulo **n** . Chaque engagement est calculé :

• soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

où **r** est un aléa produit par les moyens de production d'aléas, **r** étant tel que $0 < r < n$,

• soit en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois .

Ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D**,

  • soit en effectuant des opérations du type :

$$\mathbf{D \equiv r \,.\, Q_1}^{\mathbf{d1}} \mathbf{\,.\, Q_2}^{\mathbf{d2}} \mathbf{.\, \ldots\, Q_m}^{\mathbf{dm}} \mathbf{\bmod n}$$

  • soit en effectuant des opérations du type :

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}}^{\mathbf{d1}} \mathbf{\,.\, Q_{i,2}}^{\mathbf{d2}} \mathbf{.\, \ldots\, Q_{i,m}}^{\mathbf{dm}} \mathbf{\bmod p_i},$$

puis en appliquant la méthode des restes chinois,

Ledit dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D**. Il y a autant de réponses **D** que de défis **d** que d'engagements **R**. Chaque groupe de nombres **R, d, D** constitue un triplet noté **{R, d, D}.**

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le système selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur,

Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade, par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système comporte aussi un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte

des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

Ledit système permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion.

- **étape 2 : acte de défi d**

Le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**. Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur. Le dispositif contrôleur comporte aussi :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R,** les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement **R,** les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Cas de la preuve de l'intégrité d'un message.

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le système selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Ledit dispositif démonstrateur peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit système comporte aussi dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur.

Ledit système exécute les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de

chaque engagement **R,** pour calculer au moins un jeton **T**. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T,** via les moyens de connexion, au dispositif contrôleur. Le dispositif contrôleur comporte aussi des moyens de production de défis pour produire, après avoir reçu le jeton **T,** des défis **d** en nombre égal au nombre d'engagements **R.** Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

• **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur. Le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R',** un jeton **T'.**

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé **T'** au jeton **T** reçu.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec l'une et/ou l'autre des deux premières, le système selon l'invention est destiné à prouver la signature numérique d'un message **M,** ci-après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message **M,**
- les défis **d** et/ou les engagements **R,**
- les réponses **D** ;

Opération de signature

Ledit système est tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion et peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R,** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R.**

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

Opération de contrôle

Pour prouver l'authenticité du message **M,** une entité appelée contrôleur, contrôle le message signé.

Ledit système comporte un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif signataire.

Le dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion. Ainsi, le dispositif contrôleur dispose d'un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• cas où le dispositif contrôleur dispose des engagements R, des défis d, des réponses D,

Dans le cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\,(message, R)}$$

• cas où le dispositif contrôleur dispose des défis d et des réponses D

Dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**, les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R')}$$

• **cas où le dispositif contrôleur dispose des engagements R et des réponses D**

Dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,** les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$\mathbf{d' = h\ (message, R)}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$\mathbf{R \equiv G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . \bmod n}$$

Dispositif Terminal

L'invention concerne aussi un dispositif terminal associé à une entité. Le dispositif terminal se présente notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif terminal est destiné à prouver à un dispositif contrôleur :

- l'authenticité de l'entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n .$$

Ledit exposant v est tel que

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 .

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que :

les deux équations :

$$x^2 \equiv g_i \mathbf{mod}\ n \quad \text{et} \quad x^2 \equiv -g_i \mathbf{mod}\ n$$

n'ont pas de solution en x dans l'anneau des entiers modulo n

et tel que :

l'équation :

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

a des solutions en x dans l'anneau des entiers modulo n .

Ledit dispositif terminal comprend un dispositif témoin comportant une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les f.m composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et l'exposant public v .

Ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin, pour calculer des engagements R dans l'anneau des entiers modulo n .

Chaque engagement est calculé :

• soit en effectuant des opérations du type

$$R \equiv r^v \mathbf{mod}\ n$$

ou **r** est un aléa produit par les moyens de production d'aléas, **r** étant tel que $0 < r < n$,

• soit en effectuant des opérations du type

$$R_i \equiv r_i^{v} \bmod p_i$$

ou r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois.

Le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D**,

• soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

puis en appliquant la méthode des restes chinois.

Ledit dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D**. Il y a autant de réponses **D** que de défis **d** que d'engagements **R**. Chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}**.

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le dispositif terminal selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est

interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit dispositif démonstrateur comporte aussi des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion.

- **étapes 2 et 3 : acte de défi d, acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin. Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-

dessus.

• **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée à la première, le dispositif terminal selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif démonstrateur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion.

• **étapes 2 et 3 : acte de défi d, acte de réponse D**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer au moins un jeton **T**. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T**, via les moyens de connexion, au dispositif contrôleur.

Ledit dispositif contrôleur produit, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**.

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin.

Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec l'une ou l'autre des deux premières, le dispositif terminal selon l'invention est destiné à produire la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D**.

Ledit dispositif terminal est tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif signataire comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Opération de signature

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R,** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R.**

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion.

Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

Dispositif contrôleur

L'invention concerne aussi un dispositif contrôleur. Le dispositif contrôleur peut se présenter notamment sous la forme d'un terminal ou d'un serveur distant associé à une entité contrôleur. Le dispositif contrôleur est destiné à contrôler :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2) inconnus du dispositif contrôleur et de l'entité contrôleur associé,
- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \ \mathbf{mod\ n} \text{ ou } G_i \equiv Q_i^v \ \mathbf{mod\ n} \ ;$$

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i .

L'exposant **v** est tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1.

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur

aux **f** facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement R, acte de défi d**

Ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion.

Le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R,** des défis **d** en nombre égal au nombre d'engagements **R,** chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires.

Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

Ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion
- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement **R,** les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n ,$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus l'intégralité de chaque engagement **R,** les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^{v} / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{mod\ n} .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le dispositif contrôleur selon l'invention est destiné à prouver l'intégrité d'un message **M** associé à une entité appelée démonstrateur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement R, acte de défi d**

Ledit dispositif contrôleur comporte aussi des moyens de réception de jetons **T** provenant du dispositif démonstrateur, via les moyens de connexion. Le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu le jeton **T,** des défis **d** en nombre égal au nombre d'engagements **R,** chaque défi **d** comportant **m** entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires. Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étapes 3 et 4 : acte de réponse D, acte de contrôle**

Ledit dispositif contrôleur comporte des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion. Ledit dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'**

satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé **T'** au jeton **T** reçu.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec l'une et/ou l'autre des deux premières, le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, un message signé.

Le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage **h (message, R)**, comprend:

- le message **M**,
- des défis **d** et/ou des engagements **R**,
- des réponses **D** ;

Opération de contrôle

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associée à l'entité signataire. Ledit dispositif contrôleur reçoit le message signé du dispositif signataire, via les moyens de connexion.

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du

dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• cas où le dispositif contrôleur dispose des engagements R, des défis d, des réponses D,

Dans le cas où le dispositif contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,** les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R,** les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage :

$$\mathbf{d = h\ (message, R)}$$

• cas où le dispositif contrôleur dispose des défis d et des réponses D

Dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D,** les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D,** des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R')}$$

• cas où le dispositif contrôleur dispose des engagements R et des réponses D

Dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,** les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$\mathbf{d' = h\ (message, R)}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$\mathbf{R \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n}$$

Description

Rappelons l'objectif de la technologie GQ : l'authentification dynamique d'entités et de messages associés, ainsi que la signature numérique de messages.

La version classique de la technologie GQ fait appel à la technologie RSA. Mais, si la technologie RSA dépend bel et bien de la factorisation, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites « multiplicatives » contre diverses normes de signature numérique mettant en œuvre la technologie RSA.

Dans le cadre de la technologie GQ2, la présente partie de l'invention porte plus précisément sur l'utilisation des jeux de clés GQ2 dans le cadre de l'authentification dynamique et de la signature numérique. La technologie GQ2 ne fait pas appel à la technologie RSA. L'objectif est double : d'une part, améliorer les performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La clé privée GQ2 est la factorisation du module n. Toute attaque au niveau de striplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 concurrence la technologie RSA.

La technologie GQ2 utilise un ou plusieurs petits nombres entiers plus grands que 1, disons m petits nombres entiers ($m \geq 1$) appelés « nombres de base » et notés par g_i. Les nombres de base étant fixés de g_1 à g_m avec $m \geq 1$, une clé publique de vérification $\langle v, n \rangle$ est choisie de la manière suivante. L'exposant public de vérification v est 2^k où k est un petit nombre entier plus grand que 1 ($k \geq 2$). Le module public n est le produit d'au moins deux facteurs premiers plus grands que les nombres de base, disons f facteurs premiers ($f \geq 2$) notés par p_j, de $p_1 \ldots p_f$. Les f facteurs premiers sont choisis

de façon à ce que le module public n ait les propriétés suivantes par rapport à chacun des m nombres de base de g_1 à g_m.

- D'une part, les équations (1) et (2) n'ont pas de solution en x dans l'anneau des entiers modulo n, c'est-à-dire que g_i et $-g_i$ sont deux résidus non quadratiques (mod n).

$$x^2 \equiv g_i \pmod{n} \qquad (1)$$

$$x^2 \equiv -g_i \pmod{n} \qquad (2)$$

- D'autre part, l'équation (3) a des solutions en x dans l'anneau des entiers modulo n.

$$x^{2^k} \equiv g_i^2 \pmod{n} \qquad (3)$$

La clé publique de vérification $\langle v, n \rangle$ étant fixée selon les nombres de base de g_1 à g_m avec $m \geq 1$, chaque nombre de base g_i détermine un couple de valeurs GQ2 comprenant une valeur publique G_i et une valeur privée Q_i: soit m couples notés de G_1 Q_1 à G_m Q_m. La valeur publique G_i est le carré du nombre de base g_i: soit $G_i = g_i^2$. La valeur privée Q_i est une des solutions à l'équation (3) ou bien l'inverse (mod n) d'une telle solution.

De même que le module n se décompose en f facteurs premiers, l'anneau des entiers modulo n se décompose en f corps de Galois, de CG(p_1) à CG(p_f). Voici les projections des équations (1), (2) et (3) dans CG(p_j).

$$x^2 \equiv g_i \pmod{p_j} \qquad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_j} \qquad (2.a)$$

$$x^{2^k} \equiv g_i^2 \pmod{p_j} \qquad (3.a)$$

Chaque valeur privée Q_i peut se représenter de manière unique par f composantes privées, une par facteur premier : $Q_{i,j} \equiv Q_i \pmod{p_j}$. Chaque composante privée $Q_{i,j}$ est une solution à l'équation (3.a) ou bien l'inverse (mod p_j) d'une telle solution. Après que toutes les solutions possibles à chaque équation (3.a) aient été calculées, la technique des restes chinois permet d'établir toutes les valeurs possibles pour chaque valeur privée Q_i à partir de f composantes de $Q_{i,1}$ à $Q_{i,f}$: Q_i = Restes Chinois ($Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$)

de manière à obtenir toutes les solutions possibles à l'équation (3).

Voici la technique des restes chinois : soient deux nombres entiers positifs premiers entre eux a et b tels que $0 < a < b$, et deux composantes X_a de 0 à a–1 et X_b de 0 à b–1 ; il s'agit de déterminer X = Restes Chinois (X_a, X_b), c'est-à-dire, le nombre unique X de 0 à $a.b$–1 tel que $X_a \equiv X \pmod{a}$ et $X_b \equiv X \pmod{b}$. Voici le paramètre des restes chinois : $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. Voici l'opération des restes chinois : $\varepsilon \equiv X_b \pmod{a}$; $\delta = X_a - \varepsilon$; si δ est négatif, remplacer δ par $\delta + a$; $\gamma \equiv \alpha \,.\, \delta \pmod{a}$; $X = \gamma \,.\, b + X_b$.

Lorsque les facteurs premiers sont rangés dans l'ordre croissant, du plus petit p_1 au plus grand p_f, les paramètres des restes chinois peuvent être les suivants (il y en a f–1, c'est-à-dire, un de moins que de facteurs premiers). Le premier paramètre des restes chinois est $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. Le second paramètre des restes chinois est $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. Le i ième paramètre des restes chinois est $\lambda \equiv \{p_1.p_2. \ldots p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$. Et ainsi de suite. Ensuite, en f–1 opérations des restes chinois, on établit un premier résultat (mod p_2 fois p_1) avec le premier paramètre, puis, un second résultat (mod $p_1.p_2$ fois p_3) avec le second paramètre, et ainsi de suite, jusqu'à un résultat (mod $p_1. \ldots p_{f-1}$ fois p_f), c'est-à-dire, (mod n).

Il y a plusieurs représentations possibles de la clé privée GQ2, ce qui traduit **le polymorphisme de la clé privée GQ2**. Les diverses représentations s'avèrent équivalentes : elles se ramènent toutes à la connaissance de la factorisation du module n qui est la véritable clé privée GQ2. Si la représentation affecte bien le comportement de l'entité qui signe ou qui s'authentifie, elle n'affecte pas le comportement de l'entité qui contrôle.

Voici les trois principales représentations possibles de la clé privée GQ2. 1) La représentation classique en technologie GQ consiste à stocker m valeurs privées Q_i et la clé publique de vérification $\langle v, n \rangle$; en technologie GQ2, cette représentation est concurrencée par les deux suivantes. 2) La représentation optimale en termes de charges de travail consiste à stocker

l'exposant public v, les f facteurs premiers p_j, $m.f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois. 3) La représentation optimale en termes de taille de clé privée consiste à stocker l'exposant public v, les m nombres de base g_i et les f facteurs premiers p_j, puis, à commencer chaque utilisation en établissant ou bien m valeurs privées Q_i et le module n pour se ramener à la première représentation, ou bien $m.f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois pour se ramener à la seconde.

Les entités qui signent ou s'authentifient peuvent toutes utiliser les mêmes nombres de base ; sauf contre indication, les m nombres de base de g_1 à g_m peuvent alors avantageusement être les m premiers nombres premiers.

Parce que la sécurité du mécanisme d'authentification dynamique ou de signature numérique équivaut à la connaissance d'une décomposition du module, la technologie GQ2 ne permet pas de distinguer simplement deux entités utilisant le même module. Généralement, chaque entité qui s'authentifie ou signe dispose de son propre module GQ2. Toutefois, on peut spécifier des modules GQ2 à quatre facteurs premiers dont deux sont connus d'une entité et les deux autres d'une autre.

Voici un premier jeu de clés GQ2 avec $\boldsymbol{k = 6}$, soit $v = 64$, $\boldsymbol{m = 3}$, soit trois nombres de base : $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, et $\boldsymbol{f = 3}$, soit un module à trois facteurs premiers : deux congrus à 3 (mod 4) et un à 5 (mod 8). Notons que $g = 2$ est incompatible avec un facteur premier congru à 5 (mod 8).

p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833

p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B

p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9
02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144
CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD

$Q_{1,1}$ = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE

$Q_{2,1}$ = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89

$Q_{3,1}$ = 6FB3B9C05A03D7CADA9A3425571EF5ECC54D7A7B6F

$Q_{1,2}$ = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502

$Q_{2,2}$ = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E

$Q_{3,2}$ = FDC4A8E53E185A4BA793E93BEE5C636DA731BDCA4E

$Q_{1,3}$ = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE

$Q_{2,3}$ = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877

$Q_{3,3}$ = 01682D490041913A4EA5B80D16B685E4A6DD88070501

Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8
C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A
C74D9743435AB4D7CF0FF6557

Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4
DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8
82288273ADE67353A5BC316C093

Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A
AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197
697238537FE7A0195C5E8373EB74D

Voici un second jeu de clés GQ2, avec $k = 9$, soit $v = 512$, $m = 2$, soit deux nombres de base : $g_1 = 2$ et $g_2 = 3$, et $f = 3$, soit un module à trois facteurs premiers congrus à 3 (mod 4).

p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB

p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7

p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D
6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49
761B276A8E6B6977A21D51669D039F1D7

$Q_{1,1}$ = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1

$Q_{2,1}$ = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E

$Q_{1,2}$ = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A

$Q_{2,2}$ = 045ECB881387582E7C556887784D2671CA118E22FCF2

$Q_{1,3}$ = B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982

$Q_{2,3}$ = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB

Q_1 = 27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C
35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6
EDDA092D0CF108D0AB708405DA46

Q_2 = 230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64
9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6
F11F19874DE7DC5D1DF2A9252D

Authentification dynamique

Le mécanisme d'authentification dynamique est destiné à prouver à une entité appelée **contrôleur** l'authenticité d'une autre entité appelée **démonstrateur** ainsi que l'authenticité d'un éventuel message associé *M*, de sorte que le contrôleur s'assure qu'il s'agit bien du démonstrateur et éventuellement que lui et le démonstrateur parlent bien du même message *M*. Le message associé *M* est optionnel, ce qui signifie qu'il peut être vide.

Le mécanisme d'authentification dynamique est une séquence de quatre actes : un acte d'engagement, un acte de défi, un acte de réponse et un acte de contrôle. Le démonstrateur joue les actes d'engagement et de réponse. Le contrôleur joue les actes de défi et de contrôle.

Au sein du démonstrateur, on peut isoler un témoin, de manière à isoler les paramètres et les fonctions les plus sensibles du démonstrateur, c'est-à-dire, la production des engagements et des réponses. Le témoin dispose du paramètre *k* et de la clé privée GQ2, c'est-à-dire, de la factorisation du module *n* selon l'une des trois représentations évoquées ci-dessus : • les *f* facteurs premiers et les *m* nombres de base, • les *m.f* composantes privées, les *f* facteurs premiers et *f*–1 paramètres des restes chinois, • les *m* valeurs privées et le module *n*.

Le témoin peut correspondre à une réalisation particulière, par exemple,
• une carte à puce reliée à un PC formant ensemble le démonstrateur, ou

encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce. Le témoin ainsi isolé est semblable au témoin défini ci-après au sein du signataire. A chaque exécution du mécanisme, le témoin produit un ou plusieurs engagements R, puis, autant de réponses D à autant de défis d. Chaque ensemble $\{R, d, D\}$ constitue un **triplet GQ2**.

Outre qu'il comprend le témoin, le démonstrateur dispose également, le cas échéant, d'une fonction de hachage et d'un message M.

Le contrôleur dispose du module n et des paramètres k et m ; le cas échéant, il dispose également de la même fonction de hachage et d'un message M'. Le contrôleur est apte à reconstituer un engagement R' à partir de n'importe quel défi d et de n'importe quelle réponse D. Les paramètres k et m renseignent le contrôleur. Faute d'indication contraire, les m nombres de base de g_1 à g_m sont les m premiers nombres premiers. Chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m: un par nombre de base. Chaque défi élémentaire de d_1 à d_m doit prendre une valeur de 0 à $2^{k-1}-1$ (les valeurs de $v/2$ à $v-1$ ne sont pas utilisées). Typiquement, chaque défi est codé par m fois $k-1$ bits (et non pas m fois k bits). Par exemple, avec $k = 6$ et $m = 3$ et les nombres de base 3, 5 et 7, chaque défi comporte 15 bits transmis sur deux octets ; avec $k = 9$, $m = 2$ et les nombres de base 2 et 3, chaque défi comporte 16 bits transmis sur deux octets. Lorsque les $(k-1).m$ défis possibles sont également probables, la valeur $(k-1).m$ détermine la sécurité apportée par chaque triplet GQ2 : un imposteur qui, par définition, ne connaît pas la factorisation du module n a exactement une chance de succès sur $2^{(k-1).m}$. Lorsque $(k-1).m$ vaut de 15 à 20, un triplet suffit à assurer raisonnablement l'authentification dynamique. Pour atteindre n'importe quel niveau de sécurité, on peut produire des triplets en parallèle ; on peut également en produire en séquence, c'est-à-dire, répéter l'exécution du mécanisme.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Voici un exemple avec le premier jeu de clés avec $k = 6$.

r = B8AD426C1AC0165E94B894AC2437C1B1797EF562CFA53A4AF8
43131FF1C89CFDA131207194710EF9C010E8F09C60D9815121981260
919967C3E2FB4B4566088E

R = FFDD736B666F41FB771776D9D50DB7CDF03F3D976471B25C56
D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C21210C6B04
49CC4292E5DD2BDB00828AF18

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées Q_{ij}, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i), il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Voici un exemple avec le second jeu de clés avec $k = 9$.

r_1 = B0418EABEBADF0553A28903F74472CD49EE8C82D86

R_1 = 022B365F0BEA8E157E94A9DEB0512827FFD5149880F1

r_2 = 75A8DA8FE0E60BD55D28A218E31347732339F1D667

R_2 = 057E43A242C485FC20DEEF291C774CF1B30F0163DEC2

r_3 = 0D74D2BDA5302CF8BE2F6D406249D148C6960A7D27

R_3 = 06E14C8FC4DD312BA3B475F1F40CF01ACE2A88D5BB3C

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

R = Restes Chinois(R_1, R_2, ... R_f)

R = 28AA7F12259BFBA81368EB49C93EEAB3F3EC6BF73B0EBD7
D3FC8395CFA1AD7FC0F9DAC169A4F6F1C46FB4C3458D1E37C9
9123B56446F6C928736B17B4BA4A529

Dans les deux cas, le démonstrateur transmet au contrôleur tout ou partie de chaque engagement ***R***, ou bien, un code de hachage ***H*** obtenu en hachant chaque engagement ***R*** et un message ***M***.

2) L'acte de défi consiste à tirer au hasard un ou plusieurs défis d composés chacun de m défis élémentaires d_1 d_2 ... d_m ; chaque défi élémentaire d_i prend l'une des valeurs de 0 à $v/2-1$.

$$d = d_1\ d_2 \ldots\ d_m$$

Voici un exemple pour le premier jeu de clés avec $k = 6$ et $m = 3$.

$$d_1 = 10110 = 22 = \text{'16'}\ ;\ d_2 = 00111 = 7\ ;\ d_3 = 00010 = 2,$$
$$d = 0\ ||\ d_1\ ||\ d_2\ ||\ d_3 = 01011000\ 11100010 = 58\ \text{E2}$$

Voici un exemple pour le second jeu de clés avec $k = 9$ et $m = 2$.

$$d = d_1\ ||\ d_2 = 58\ \text{E2} = \text{soit en décimal, 88 et 226}$$

Le contrôleur transmet au démonstrateur chaque défi ***d***.

3) L'acte de réponse comporte les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les valeurs privées selon les défis élémentaires.

$$X \equiv Q_1^{d_1}.Q_2^{d_2}...Q_m^{d_m} \pmod{n}$$
$$D \equiv r.X \pmod{n}$$

Voici un exemple pour le premier jeu de clés.

D = FF257422ECD3C7A03706B9A7B28EE3FC3A4E974AEDCDF386
5EEF38760B859FDB5333E904BBDD37B097A989F69085FE8EF6480
A2C6A290273479FEC9171990A17

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f

composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1}.Q_{2,i}^{d_2}...Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i.X_i \pmod{p_i}$$

Voici un exemple pour le second jeu de clés.

$D_1 = r_1 \cdot Q_{1,1}^{d1} \cdot Q_{2,1}^{d2} \pmod{p_1} =$

02660ADF3C73B6DC15E196152322DDE8EB5B35775E38

$D_2 = r_2 \cdot Q_{1,2}^{d1} \cdot Q_{2,2}^{d2} \pmod{p_2} =$

04C15028E5FD1175724376C11BE77052205F7C62AE3B

$D_3 = r_3 \cdot Q_{1,3}^{d1} \cdot Q_{2,3}^{d2} \pmod{p_3} =$

0903D20D0C306C8EDA9D8FB5B3BEB55E061AB39CCF52

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

D = 85C3B00296426E97897F73C7DC6341FB8FFE6E879AE12EF1F36

4CBB55BC44DEC437208CF530F8402BD9C511F5FB3B3A309257A00

195A7305C6FF3323F72DC1AB

Dans les deux cas, le démonstrateur transmet chaque réponse $\boldsymbol{D}$ au contrôleur.

4) L'acte de contrôle consiste à contrôler que chaque triplet $\{R, d, D\}$ vérifie une équation du type suivant pour une valeur non nulle,

$$R.\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

ou bien, à rétablir chaque engagement : aucun ne doit être nul.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Eventuellement, le contrôleur calcule ensuite un code de hachage H' en

hachant chaque engagement rétabli R' et un message M'. L'authentification dynamique est réussie lorsque le contrôleur retrouve ainsi ce qu'il a reçu à l'issue de l'acte d'engagement, c'est-à-dire, tout ou partie de chaque engagement R, ou bien, le code de hachage H.

Par exemple, une séquence d'opérations élémentaires transforme la réponse D en un engagement R'. La séquence comprend k carrés (mod n) séparés par k–1 divisions ou multiplications (mod n) par des nombres de base. Pour la i ième division ou multiplication, qui s'effectue entre le i ième carré et le i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m.

Voici un exemple pour le premier jeu de clés.

D^2 (mod n) = FD12E8E1F1370AEC9C7BA2E05C80AD2B692D341D46F3
2B93948715491F0EB091B7606CA1E744E0688367D7BB998F7B73D5F7
FDA95D5BD6347DC8B978CA217733

3 . D^2 (mod n) = F739B708911166DFE715800D8A9D78FC3F332FF622D
3EAB8E7977C68AD44962BEE4DAE3C0345D1CB34526D3B67EBE8BF
987041B4852890D83FC6B48D3EF6A9DF

3^2 . D^4 (mod n) = 682A7AF280C49FE230BEE354BF6FFB30B7519E3C8
92DD07E5A781225BBD33920E5ADABBCD7284966D71141EAA17AF
8826635790743EA7D9A15A33ACC7491D4A7

3^4 . D^8 (mod n) = BE9D828989A2C184E34BA8FE0F384811642B7B548F
870699E7869F8ED851FC3DB3830B2400C516511A0C28AFDD210EC3
939E69D413F0BABC6DEC441974B1A291

3^5 . 5 . D^8 (mod n) = 2B40122E225CD858B26D27B768632923F2BBE5
DB15CA9EFA77EFA667E554A02AD1A1E4F6B59BD9E1AE4A537D
4AC1E89C2235C363830EBF4DB42CEA3DA98CFE00

3^{10} . 5^2 . D^{16} (mod n) = BDD3B34C90ABBC870C604E27E7F2E9DB2D383
68EA46C931C66F6C7509B118E3C162811A98169C30D4DEF768397DD

B8F6526B6714218DEB627E11FACA4B9DB268

$3^{11} . 5^3 . 7 . D^{16} \pmod{n}$ = DBFA7F40D338DE4FBA73D42DBF427BBF195
C13D02AB0FA5F8C8DDB5025E34282311CEF80BACDCE5D0C433444
A2AF2B15318C36FE2AE02F3C8CB25637C9AD712F

$3^{22} . 5^6 . 7^2 . D^{32} \pmod{n}$ = C60CA9C4A11F8AA89D9242CE717E3DC6C1
A95D5D09A2278F8FEE1DFD94EE84D09D000EA8633B53C4A0E7F0A
EECB70509667A3CB052029C94EDF27611FAE286A7

$3^{22} . 5^7 . 7^2 . D^{32} \pmod{n}$ = DE40CB6B41C01E722E4F312AE7205F18CDD
0303EA52261CB0EA9F0C7E0CD5EC53D42E5CB645B6BB1A3B00C77
886F4AC5222F9C863DACA440CF5F1A8E374807AC

$3^{44} . 5^{14} . 7^4 . D^{64} \pmod{n}$, c'est-à-dire, $3^{2C} . 5^E . 7^4 . D^{40} \pmod{n}$ avec les exposants en hexa = FFDD736B666F41FB771776D9D50DB7CDF03F3D9
76471B25C56D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C
21210C6B0449CC4292E5DD2BDB00828AF18

On retrouve bien l'engagement ***R***. L'authentification est réussie.

Voici un exemple pour le second jeu de clés.

$D^2 \pmod{n}$ = C66E585D8F132F7067617BC6D00BA699ABD74FB9D13E
24E6A6692CC8D2FC7B57352D66D34F5273C13F20E3FAA228D70AEC
693F8395ACEF9206B172A8A2C2CCBB

$3 . D^2 \pmod{n}$ = 534C6114D385C3E15355233C5B00D09C2490D1B8D8E
D3D59213CB83EAD41C309A187519E5F501C4A45C37EB2FF38FBF20
1D6D138F3999FC1D06A2B2647D48283

$3^2 . D^4 \pmod{n}$ = A9DC8DEA867697E76B4C18527DFFC49F4658473D03
4EC1DDE0EB21F6F65978BE477C4231AC9B1EBD93D5D49422408E47
15919023B16BC3C6C46A92BBD326AADF

$2 . 3^3 . D^4 \pmod{n}$ = FB2D57796039DFC4AF9199CAD44B66F257A1FF
3F2BA4C12B0A8496A0148B4DFBAFE838E0B5A7D9FB4394379D72A
107E45C51FCDB7462D03A35002D29823A2BB5

$2^2 . 3^6 . D^8 \pmod{n}$ = 4C210F96FF6C77541910623B1E49533206DFB9E91

6521F305F12C5DB054D4E1BF3A37FA293854DF02B49283B6DE5E5D
82ACB23DAF1A0D5A721A1890D03A00BD8

$2^2 \cdot 3^7 \cdot D^8 \pmod{n}$ = E4632EC4FE4565FC4B3126B15ADBF996149F2D
BB42F65D911D3851910FE7EA53DAEA7EE7BA8FE9D081DB78B249
B1B18880616B90D4E280F564E49B270AE02388

$2^4 \cdot 3^{14} \cdot D^{16} \pmod{n}$ = ED3DDC716AE3D1EA74C5AF935DE814BCC
2C78B12A6BB29FA542F9981C5D954F53D153B9F0198BA82690EF
665C17C399607DEA54E218C2C01A890D422EDA16FA3

$2^5 \cdot 3^{14} \cdot D^{16} \pmod{n}$ = DA7C64E0E8EDBE9CF823B71AB13F17E1161487
6B000FBB473F5FCBF5A5D8D26C7B2A05D03BDDD588164E562D0F5
7AE94AE0AD3F35C61C0892F4C91DC0B08ED6F

$2^{10} \cdot 3^{28} \cdot D^{32} \pmod{n}$ = 6ED6AFC5A87D2DD117B0D89072C99FB9DC9
5D558F65B6A1967E6207D4ADBBA32001D3828A35069B256A07C3D
722F17DA30088E6E739FBC419FD7282D16CD6542

$2^{11} \cdot 3^{28} \cdot D^{32} \pmod{n}$ = DDAD5F8B50FA5BA22F61B120E5933F73B92
BAAB1ECB6D432CFCC40FA95B77464003A705146A0D364AD40F8
7AE45E2FB460111CDCE73F78833FAE505A2D9ACA84

$2^{22} \cdot 3^{56} \cdot D^{64} \pmod{n}$ = A466D0CB17614EFD961000BD9EABF4F021
36F8307101882BC1764DBAACB715EFBF5D8309AE001EB5DEDA
8F000E44B3D4578E5CA55797FD4BD1F8E919BE787BD0

$2^{44} \cdot 3^{112} \cdot D^{128} \pmod{n}$ = 925B0EDF5047EFEC5AFABDC03A830919761
B8FBDD2BF934E2A8A31E29B976274D513007EF1269E4638B4F65F
8FDEC740778BDC178AD7AF2968689B930D5A2359

$2^{44} \cdot 3^{113} \cdot D^{128} \pmod{n}$ = B711D89C03FDEA8D1F889134A4F809B3F2D
8207F2AD8213D169F2E99ECEC4FE08038900F0C203B55EE4F4C803
BFB912A04F11D9DB9D076021764BC4F57D47834

$2^{88} \cdot 3^{226} \cdot D^{256} \pmod{n}$ = 41A83F119FFE4A2F4AC7E5597A5D0BEB4D4C
08D19E597FD034FE720235894363A19D6BC5AF323D24B1B7FCFD8D
FCC628021B4648D7EF757A3E461EF0CFF0EA13

$2^{176} . 3^{452} . D^{512} \pmod{n}$, soit $4^{88} . 9^{226} . D^{512} \pmod{n}$ = 28AA7F12259BFBA8 1368EB49C93EEAB3F3EC6BF73B0EBD7D3FC8395CFA1AD7FC0F9D AC169A4F6F1C46FB4C3458D1E37C99123B56446F6C928736B17B4BA 4A529

On retrouve bien l'engagement R. L'authentification est réussie.

Signature numérique

Le mécanisme de signature numérique permet à une entité appelée **signataire** de produire des messages signés et à une entité appelée **contrôleur** de vérifier des messages signés. Le message M est une séquence binaire quelconque : il peut être vide. Le message M est signé en lui adjoignant un appendice de signature qui comprend un ou plusieurs engagements et / ou défis, ainsi que les réponses correspondantes.

Le contrôleur dispose de la même fonction de hachage, des paramètres k et m et du module n. Les paramètres $\boldsymbol{k}$ et $\boldsymbol{m}$ renseignent le contrôleur. D'une part, chaque défi élémentaire, de d_1 à d_m, doit prendre une valeur de 0 à $2^{k-1}-1$ (les valeurs de $v/2$ à $v-1$ ne sont pas utilisées). D'autre part, chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m, autant que de nombres de base. En outre, faute d'indication contraire, les m nombres de base, de g_1 à g_m, sont les m premiers nombres premiers. Avec $(k-1).m$ valant de 15 à 20, on peut signer avec quatre triplets GQ2 produits en parallèle ; avec $(k-1).m$ valant 60 ou plus, on peut signer avec un seul triplet GQ2. Par exemple, avec $k = 9$ et $m = 8$, un seul triplet GQ2 suffit ; chaque défi comporte huit octets et les nombres de base sont 2, 3, 5, 7, 11, 13, 17 et 19.

L'opération de signature est une séquence de trois actes : un acte d'engagement, un acte de défi et un acte de réponse. Chaque acte produit un ou plusieurs triplets GQ2 comprenant chacun : un engagement R ($\neq 0$), un défi d composé de m défis élémentaires notés par d_1, d_2, ... d_m et une réponse D ($\neq 0$).

Le signataire dispose d'une fonction de hachage, du paramètre k et de la clé

privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. **Au sein du signataire, on peut isoler un témoin qui exécute les actes d'engagement et de réponse**, de manière à isoler les fonctions et les paramètres les plus sensibles du démonstrateur. Pour calculer engagements et réponses, le témoin dispose du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. Le témoin ainsi isolé est semblable au témoin défini au sein du démonstrateur. Il peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le signataire, ou encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i), il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \ldots R_f)$$

2) L'acte de défi consiste à hacher tous les engagements R et le message à

signer M pour obtenir un code de hachage à partir duquel le signataire forme un ou plusieurs défis comprenant chacun m défis élémentaires ; chaque défi élémentaire prend une valeur de 0 à $v/2-1$; par exemple, avec $k = 9$ et $m = 8$, chaque défi comporte huit octets. Il y a autant de défis que d'engagements.

$$d = d_1\ d_2\ \ldots\ d_m, \text{ extraits du résultat Hash}(M, R)$$

3) L'acte de réponse comporte les opérations suivantes.

Lorsque la témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les valeurs privées selon les défis élémentaires.

$$X \equiv Q_1^{d_1}.Q_2^{d_2}...Q_m^{d_m} \pmod{n}$$
$$D \equiv r.X \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1}.Q_{2,i}^{d_2}...Q_{m,i}^{d_m} \pmod{p_i}$$
$$D_i \equiv r_i.X_i \pmod{p_i}$$

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

Le signataire signe le message *M* en lui adjoignant un appendice de signature comprenant :

- ou bien, chaque triplet GQ2, c'est-à-dire, chaque engagement R, chaque défi d et chaque réponse D,
- ou bien, chaque engagement R et chaque réponse D correspondante,
- ou bien, chaque défi d et chaque réponse D correspondante.

Le déroulement de l'opération de vérification dépend du contenu de l'appendice de signature. On distingue les trois cas.

Au cas où l'appendice comprend un ou plusieurs triplets, l'opération de contrôle comporte deux processus indépendants dont la chronologie est indifférente. Le contrôleur accepte le message signé si et seulement si les deux conditions suivantes sont remplies.

D'une part, chaque triplet doit être cohérent (une relation appropriée du type suivant doit être vérifiée) et recevable (la comparaison doit se faire sur une valeur non nulle).

$$R.\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Par exemple, on transforme la réponse D par une séquence d'opérations élémentaires : k carrés (mod n) séparés par k–1 multiplications ou divisions (mod n) par des nombres de base. Pour la i ième multiplication ou division, qui s'effectue entre le i ième carré et le i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, … jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m. On doit ainsi retrouver chaque engagement R présent dans l'appendice de signature.

D'autre part, le ou les triplets doivent être liés au message M. En hachant tous les engagements R et le message M, on obtient un code de hachage à partir duquel on doit retrouver chaque défi d.

$d = d_1\ d_2 \ldots\ d_m$, identiques à ceux extraits du résultat Hash(M, R)

Au cas où l'appendice ne comprend pas de défi, l'opération de contrôle commence par la reconstitution de un ou plusieurs défis d' en hachant tous les engagements R et le message M.

$d' = d'_1\ d'_2 \ldots\ d'_m$, extraits du résultat Hash(M, R)

Ensuite, le contrôleur accepte le message signé si et seulement si chaque triplet est cohérent (une relation appropriée du type suivant est vérifiée) et

recevable (la comparaison se fait sur une valeur non nulle).

$$R.\prod_{i=1}^{m} G_i^{d'i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d'i} \pmod{n}$$

Au cas où l'appendice ne comprend pas d'engagement, l'opération de contrôle commence par la reconstitution de un ou plusieurs engagements R' selon une des deux formules suivantes, celle qui est appropriée. Aucun engagement rétabli ne doit être nul.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Ensuite, le contrôleur doit hacher tous les engagements R' et le message M de façon à reconstituer chaque défis d.

$d = d_1\ d_2 \ldots d_m$, identiques à ceux extraits du résultat Hash(M, R')

Le contrôleur accepte le message signé si et seulement si chaque défi reconstitué est identique au défi correspondant figurant en appendice.

Dans la présente demande, on a montré qu'il existait des couples de valeurs privée Q et publique G permettant de mettre en œuvre le procédé, le système et le dispositif selon l'invention destiné à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Dans la demande pendante déposée le même jour que la présente demande par France Télécom, TDF et la Société Math RiZK et ayant pour inventeurs Louis Guillou et Jean-Jacques Quisquater, on a décrit un procédé pour produire des jeux de clés GQ2, à savoir, des modules n et des couples de valeurs publique G et privée Q dans le cas où l'exposant v est égal à 2^k. Elle est incorporée ici par référence.

Revendications

1. Procédé destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n ;$$

ledit exposant **v** étant tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$; le nombre de base g_i étant tel que :

les deux équations :

$$x^2 \equiv g_i \mathbf{mod}\ n \qquad \text{et} \qquad x^2 \equiv -g_i \mathbf{mod}\ n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

a des solutions en x dans l'anneau des entiers modulo **n** ;

ledit procédé met en œuvre selon les étapes suivantes une entité appelée témoin disposant des **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs

privées Q_i et de l'exposant public **v** ;

- le témoin calcule des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé :

• soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

où **r** est un aléa tel que $0 < r < n$,

• soit

•• en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \dots r_t\}$,

•• puis en appliquant la méthode des restes chinois ;

- le témoin reçoit un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ; le témoin calcule à partir de chaque défi **d** une réponse **D**,

• soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \dots Q_m^{dm} \bmod n$$

• soit

•• en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \dots Q_{i,m}^{dm} \bmod p_i$$

•• puis en appliquant la méthode des restes chinois ;

ledit procédé étant tel qu'il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}**.

2. Procédé selon la revendication 1 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ladite entité démonstrateur comprenant le témoin ;

lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

• **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,
- le démonstrateur transmet au contrôleur tout ou partie de chaque engagement **R,**

• **étape 2 : acte de défi d**

- le contrôleur, après avoir reçu tout ou partie de chaque engagement **R,** produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

• **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où le démonstrateur a transmis une partie de chaque engagement **R,** le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou a une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n ,$$

le contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** qui lui a été transmis,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement **R,** le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifie que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou a une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{mod\ n} .$$

3. Procédé selon la revendication 1 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur, ladite entité démonstrateur comprenant le témoin ;
lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

- **étape 2 : acte de défi d**

- le démonstrateur applique une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**,
- le démonstrateur transmet le jeton **T** au contrôleur,
- le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

- **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

- **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,
- le contrôleur, disposant des m valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \mathbf{\ mod\ n}$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{\ mod\ n}$$

- puis le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement

reconstruit **R'** pour reconstruire le jeton **T'**,

- puis le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis.

4. Procédé selon la revendication 1 destiné à produire la signature numérique d'un message **M** par une entité appelée entité signataire, ladite entité signataire comprenant le témoin ;

Opération de signature

ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

- **étape 2 : acte de défi d**

- le signataire applique une fonction de hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour obtenir un train binaire,
- le signataire extrait de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

- **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1.

5. Procédé selon la revendication 4 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

Opération de contrôle

ladite entité contrôleur disposant du message signé exécute une opération

de contrôle en procédant comme suit :

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,**

•• le contrôleur vérifie que les engagements **R,** les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

•• le contrôleur vérifie que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

dans le cas où le contrôleur dispose des défis **d** et des réponses **D,**

•• le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D,** des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

•• le contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R')}$$

• cas où le contrôleur dispose des engagements R et des réponses D

dans le cas où le contrôleur dispose des engagements **R** et des réponses **D,**

•• le contrôleur applique la fonction de hachage et reconstruit **d'**

$$\mathbf{d' = h\ (message, R)}$$

•• le contrôleur vérifie que les engagements **R,** les défis **d'** et les réponses **D,** satisfont à des relations du type :

$$R \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n$$

6. Système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^{\,v} \equiv 1 \cdot \bmod n \text{ ou } G_i \equiv Q_i^{\,v} \bmod n ;$$

ledit exposant **v** étant tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$; le nombre de base g_i étant tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** ;

ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire

à microprocesseur,

le dispositif témoin comporte

- une zone mémoire contenant les **f** facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public **n** et/ou les **m** valeurs privées Q_i et/ou les **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et l'exposant public **v** ;

ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé :

• soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

où **r** est un aléa produit par les moyens de production d'aléas, **r** étant tel que $0 < r < n$,

• soit en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D**,

• soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

puis en appliquant la méthode des restes chinois,

- des moyens de transmission pout transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R,** chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

7. Système selon la revendication 6 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur,

ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés

les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

- **étape 2 : acte de défi d**

le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R,** des défis **d** en nombre égal au nombre d'engagements **R,**

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

- **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

- **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R,** les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n ,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement **R,** les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

8. Système selon la revendication 6 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la

forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

ledit système permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

- **étape 2 : acte de défi d**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R,** pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T,** via les moyens de connexion, au dispositif contrôleur,

le dispositif contrôleur comporte aussi des moyens de production de défis pour produire, après avoir reçu le jeton **T,** des défis **d** en nombre égal au nombre d'engagements **R,**

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après

désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**,

le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé **T'** au jeton **T** reçu.

9. Système selon la revendication 6 destiné à produire la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire ;

le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

Opération de signature

ledit système étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit système permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion,

- **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R,** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R,**

- **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

10. Système selon la revendication 9 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

Opération de contrôle

ledit système étant tel qu'il comporte un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif signataire ;

le dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion, de telle sorte que le dispositif contrôleur dispose d'un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de

comparaison du dispositif contrôleur,

• cas où le dispositif contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le dispositif contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,**

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R)}$$

• cas où le dispositif contrôleur dispose des défis d et des réponses D

dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D,**

• • les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R')}$$

• cas où le dispositif contrôleur dispose des engagements R et des réponses D

dans le cas où le dispositif contrôleur dispose des engagements **R** et des

réponses **D**,

•• les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$\mathbf{d' = h\ (message, R)}$$

•• les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$\mathbf{R \equiv G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . \bmod n}$$

11. Dispositif terminal associé à une entité, se présentant notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur, destiné à prouver à un dispositif contrôleur,

- l'authenticité de l'entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$\mathbf{G_i . Q_i^v \equiv 1 . \bmod n} \text{ ou } \mathbf{G_i \equiv Q_i^v \bmod n} ;$$

ledit exposant **v** étant tel que

$$\mathbf{v = 2^k}$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$; le nombre de base g_i étant tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** ;

ledit dispositif terminal comprend un dispositif témoin comportant,

- une zone mémoire contenant les **f** facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public **n** et/ou les **m** valeurs privées Q_i et/ou les **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et l'exposant public **v** ;

ledit dispositif témoin comporte aussi

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé :

• soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

ou **r** est un aléa produit par les moyens de production d'aléas, **r** étant tel que $0 < r < n$,

• soit en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

ou r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de

réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D**,

  • soit en effectuant des opérations du type :

  $$\mathbf{D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n}$$

  • soit en effectuant des opérations du type :

  $$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i}$$

puis en appliquant la méthode des restes chinois,

- des moyens de transmission pout transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;

il y a autant de réponses **D** que de défis **d** que d'engagements **R,** chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

12. Dispositif terminal selon la revendication 11 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur,

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal

ou d'un serveur distant ;
ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,
le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,
le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

• **étapes 2 et 3 : acte de défi d, acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin,
les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle,

13. Dispositif terminal selon la revendication 11 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,
ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur

associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

- **étapes 2 et 3 : acte de défi d, acte de réponse D**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R,** pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T,** via les moyens de connexion, au dispositif contrôleur,

*(ledit dispositif contrôleur produit, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**,)*

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

14. Dispositif terminal selon la revendication 11 destiné à produire la signature numérique d'un message **M,** ci-après désigné le message signé, par une entité appelée entité signataire ;

le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ledit dispositif terminal étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif signataire comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit

dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

Opération de signature

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion,

- **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R,** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R,**

- **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

15. Dispositif contrôleur, se présentant notamment sous la forme d'un terminal ou d'un serveur distant, associé à une entité contrôleur,

destiné à contrôler :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2) inconnus du dispositif contrôleur et de l'entité contrôleur associé,
- un exposant public **v** ;

ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n ;$$

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i ,

ledit exposant **v** étant tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

ladite valeur publique G_i étant le carré g_i^2 d'un nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$; le nombre de base g_i étant tel que :

les deux équations :

$$x^2 \equiv g_i \mathbf{mod}\ n \qquad \text{et} \qquad x^2 \equiv -g_i \mathbf{mod}\ n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**

et tel que :

l'équation :

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

a des solutions en x dans l'anneau des entiers modulo **n** ;

16. Dispositif contrôleur selon la revendication 15 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée

contrôleur ;

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur ;

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

• **étapes 1 et 2 : acte d'engagement R, acte de défi d**

ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R,** des défis **d** en nombre égal au nombre d'engagements **R,** chaque défi **d** comportant **m** entiers $\mathbf{d}_i$ ci-après appelés défis élémentaires,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R

dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement **R,** les moyens de calcul du dispositif

contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n ,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où les moyens de réception du dispositif contrôleur ont reçus l'intégralité de chaque engagement **R,** les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

17. Dispositif contrôleur selon la revendication 15 destiné à prouver l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur ;

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement R, acte de défi d**

ledit dispositif contrôleur comporte aussi des moyens de réception de jetons **T** provenant du dispositif démonstrateur, via les moyens de

connexion,

le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**, chaque défi **d** comportant **m** entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires ;

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion,

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques $\mathbf{G_1}$, $\mathbf{G_2}$, ... $\mathbf{G_m}$, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$\mathbf{R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n}$$

ou à une relation du type :

$$\mathbf{R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n}$$

puis d'autre part, calculer en appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**,

le dispositif contrôleur comporte aussi

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé **T'** au jeton **T** reçu.

18. Dispositif contrôleur selon la revendication 15 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, un message signé;

le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage **h (message, R)** , comprenant :

- le message **M**,
- des défis **d** et/ou des engagements **R**,
- des réponses **D** ;

Opération de contrôle

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associée à l'entité signataire ;

ledit dispositif contrôleur ayant reçu le message signé du dispositif signataire, via les moyens de connexion,

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

• cas où le dispositif contrôleur dispose des engagements R, des défis d, des réponses D,

dans le cas où le dispositif contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,**

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

• • les moyens de calcul et de comparaison du dispositif contrôleur

vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R)}$$

• cas où le dispositif contrôleur dispose des défis d et des réponses D

dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D,**

• • les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, R')}$$

• cas où le dispositif contrôleur dispose des engagements R et des réponses D

dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,**

• • les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$\mathbf{d' = h\ (message, R)}$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$\mathbf{R \equiv G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . \bmod n}$$

Procédé destiné à prouver l'authenticité d'une entité ou l'intégrité d'un message au moyen d'un exposant public égal à une puissance de deux.

La présente invention concerne les procédés, les systèmes ainsi que les dispositifs destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Le brevet EP 0 311 470 B1 dont les inventeurs sont Louis Guillou et Jean-Jacques Quisquater décrit un tel procédé. On y fera ci-après référence en le désignant par les termes : "brevet GQ" ou " procédé GQ". Par la suite on désignera parfois par "GQ2", "invention GQ2" ou "technologie GQ2" la présente invention.

Selon le procédé GQ, une entité appelée " autorité de confiance " attribue une identité à chaque entité appelée " témoin " et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : " *Voici mon identité ; j'en connais la signature RSA.* " Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée " contrôleur " vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant le procédé GQ se déroulent " sans transfert de connaissance ". Selon le procédé GQ, le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

La technologie GQ précédemment décrite fait appel à la technologie RSA. Mais si la technologie RSA dépend bel et bien de la factorisation du module n, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites "multiplicatives" contre les diverses normes de signature numérique mettant en oeuvre la technologie RSA.

L'objectif de la technologie GQ2 est double : d'une part, améliorer les